WHAT IS CLAIMED IS:

1. An information sharing system which employs the secret key cryptography and public key cryptography, wherein a secret key can be shared within at least a group, said information sharing system comprising:

an information storing device which can at least be accessed by multiple members, and which is capable of storing the digital signature of the team master, a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data;

a storing unit for storing the public key for at least one member which is permitted to view information;

an encryption unit for encrypting input information based on said secret key cryptography which uses a secret key for encrypting information, thereby generating encrypted data;

an encrypted key generation unit for encrypting the secret key used for encryption with a public key stored in said storing unit and specified, thereby generating an encrypted key;

a transmitting unit for transmitting said plurality of encrypted keys and encrypted data to said information storing device;

a list administration unit which obtains a member list from said information storing device, judges whether or not the signature of the team master of said member list matches the specified signature, performs registration of public keys of members to be added or deletion of canceling member's public keys only in the event that said signatures match, and in the event of additional registration or cancellation, creates a new member list including at least the signature of the team master and public key

information of members, and transmits the created member list to said information storing device; and

an encryption/decryption device which has a decryption unit for obtaining desired encrypted key information and encrypted data from said information storing device, decrypting said secret key from this encrypted key information, and decrypting the obtained encrypted data with the decrypted secret key.

2. An information sharing system according to Claim 1, wherein said information storing device and said encryption/decryption device further comprise a transmission/reception notification unit for, in the event that information or data is transmitted from a sender side to a recipient side, performing transmission notification wherein the reception side is notified that information or data has been transmitted from said transmission side, and performing reception notification wherein the tranmission side is notified that information or data has been received by said reception side indeed.

3. An information sharing system according to Claim 1, wherein said encryption/decryption device further comprises an output unit for obtaining at least encrypted key information from the secret key list in said information storing device, decrypting the secret key from this encrypted key information, encrypting input information based on said secret key cryptography with the decrypted secret key so as to generate encrypted data, and outputting said encrypted data to said transmitting unit.

4. An information processing method for an information sharing

system which employs the secret key cryptography and public key cryptography, wherein a secret key can be shared within at least a group, and wherein an information storing device, which can at least be accessed by multiple members, stores the signature of the team master, a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data, said method comprising the steps of:

a step for obtaining the member list from said information storing device in the event of additional registration or cancellation of a member belonging to the group;

a step for judging whether or not the signature of the team master of said member list matches the specified signature;

a step for creating a new member list including at least the signature of the team master and public key information of members only in the event that said signatures match; and

a step for transmitting the created member list to said information storing device.

5. An information processing method for an information sharing system which employs the secret key cryptography and public key cryptography, wherein a secret key can be shared within at least a group, and wherein an information storing device, which can at least be accessed by multiple members, stores the signature of the team master, at least a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data, said method comprising the steps of:

a step for obtaining the member list from said information storing

device in the event of registering a secret key to be used by members belonging to the group;

a step for judging whether or not the signature of the team master of said member list matches the specified signature;

a step for encrypting the secret key to be registered using said specified secret key, only in the event that said signatures match; and

a step for transmitting the encrypted secret key to said information storing device.

6. An information processing method for an information sharing system according to Claim 5 which employs the secret key cryptography and public key cryptography, wherein a secret key can be shared within at least a group, and wherein an information storing device, which can at least be accessed by multiple members, stores at least the signature of the team master, a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data, said method further comprising:

a transmission/reception notification step for, in the event that information or data is transmitted from a sender side to a recipient side, performing transmission notification wherein the reception side is notified that information or data has been transmitted from said transmission side, and performing receiving notification wherein the transmission side is notified that information or data has been received by said reception side indeed.

7. An information processing method for an information sharing system which employs the secret key cryptography and public key

cryptography, wherein a secret key can be shared within at least a group, and wherein an information storing device which can at least be accessed by multiple members stores at least the signature of the team master, a group list including public key information regarding members, a secret key list including encryption key information, and encryption data, said method comprising the steps of:

a step for obtaining at least encrypted key information from the secret key list in said information storing device;

a step for decrypting a secret key from this encrypted key information;

a step for encrypting input information based on said common key cryptography with the decrypted secret key so as to generate encrypted data; and

a step for transmitting the encrypted data to said information storing device.

8. An information processing method for an information sharing system according to Claim 7 which employs the secret key cryptography and public key cryptography, wherein a secret key can be shared within at least a group, and wherein an information storing device which can at least be accessed by multiple members stores at least the signature of the team master, a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data, said method further comprising:

a transmission/reception notification step for, in the event that information or data is transmitted from a sender side to a recipient side, performing transmission notification wherein the reception side is notified

that information or data has been transmitted from said transmission side, and performing reception notification wherein the transmission side is notified that information or data has been received by said reception side indeed.

9. An information processing method for an information sharing system which employs the secret key cryptography and public key cryptography, wherein a secret key can be shared within at least a group, and wherein an information storing device which can at least be accessed by multiple members stores at least the signature of the team master, a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data, said method comprising the steps of:

a step for obtaining desired encrypted key information and encrypted data from said information storing device;

a step for decrypting the secret key from this encrypted key information; and

a step for decrypting the obtained encrypted data with the decrypted secret key.

10. An information processing method for an information sharing system according to Claim 9 which employs the secret key cryptography and public key cryptography, wherein a secret key can be shared within at least a group, and wherein an information storing device which can at least be accessed by multiple members stores at least the signature of the team master, a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data,

said method further comprising:

a transmission/reception notification step for, in the event that information or data is sent from a sender side to a recipient side, performing transmission notification wherein the reception side is notified that information or data has been transmitted from said transmission side, and performing reception notification wherein the transmission side is notified that information or data has been received by said reception side indeed.

11. A computer-readable recording medium storing programs for causing a computer to execute the following steps:

a step for obtaining a member list from an information storing device which can at least be accessed by multiple members, and which is capable of storing the signature of the team master, a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data;

a step for judging whether or not the signature of the team master of said member list matches the specified signature;

a step for creating a new member list including at least the signature of the team master and public key information of members only in the event that said signatures match; and

a step for transmitting the encrypted secret key to said information storing device.

12. A computer-readable recording medium storing programs for causing a computer to execute the following steps:

a step for obtaining a member list from an information storing device which can at least be accessed by multiple members, and which is capable of

storing the signature of the team master, a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data;

a step for judging whether or not the signature of the team master of said member list matches the specified signature;

a step for encrypting the secret key to be registered using said specified secret key, only in the event that said signatures match; and

a step for transmitting the created member list to said information storing device.

13. A computer-readable recording medium according to Claim 12 further storing programs for causing a computer to execute a transmission/reception notification step for, in the event that information or data is sent from a sender side to a recipient side, performing transmission notification wherein the reception side is notified that information or data has been transmitted from said transmission side, and performing reception notification wherein the transmission side is notified that information or data has been received by said reception side indeed.

14. A computer-readable recording medium storing programs for causing a computer to execute the following steps:

a step for obtaining at least encrypted key information from the secret key list in an information storing device which can at least be accessed by multiple members, and which is capable of storing the signature of the team master, a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data;

a step for decrypting a secret key from this encrypted key information;

a step for encrypting input information based on said secret key cryptography with the decrypted secret key so as to generate encrypted data; and

a step for transmitting the encrypted data to said information storing device.

15. A computer-readable recording medium according to Claim 14 further storing programs for causing a computer to execute a transmission/reception notification step for, in the event that information or data is sent from a sender side to a recipient side, performing transmission notification wherein the reception side is notified that information or data has been transmitted from said transmission side, and performing reception notification wherein the transmission side is notified that information or data has been received by said recipient side indeed.

16. A computer-readable recording medium storing programs for causing a computer to execute the following steps:

a step for obtaining desired encrypted key information and encrypted data from said information storing device storing at least the signature of the team master, a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data;

a step for decrypting the secret key from this encrypted key information; and

a step for decrypting the obtained encrypted data with the decrypted

secret key.

17. A computer-readable recording medium according to Claim 16 further storing programs for causing a computer to execute a transmission/reception notification step for, in the event that information or data is sent from a sender side to a recipient side, performing transmission notification wherein the reception side is notified that information or data has been transmitted from said transmission side, and performing reception notification wherein the transmission side is notified that information or data has been received by said reception side indeed.

18. An information storing device which can at least be accessed by multiple members, and which is capable of storing a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data, and which employs the secret key cryptography and public key cryptography, wherein a secret key can be shared within at least a group, said device comprising:

a member list administration unit capable of changing said member list in response to a member list manipulation request;

a secret key administration unit for registering a secret key for which a request has been made to said secret key list in response to a registration request for a secret key, this registration including the encrypted key information of said secret key, and selecting a secret key optimal for sharing information within a certain group at the time of the request, in response to the secret key request, and transmitting the selected secret key to the requesting destination; and

an encrypted data administration unit for storing the encrypted data

along with secret key information used for encrypting said data in response to the registration request of the encrypted data, and transmitting the relevant stored encrypted data and secret key information to the requesting destination in response to the request for obtaining encrypted data.

19. An information storing device according to Claim 18, wherein said member list administration unit and secret key administration unit change said member list and secret key list so that in the event of newly registering a member to a certain group, information shared by the group before the time of registration can be read.

20. An information storing device according to Claim 18, wherein said member list administration unit and secret key administration unit change said member list and secret key list so that in the event of deleting a member from a certain group, information shared by the group after the member is deleted cannot be read by the deleted member.

21. An information processing method for an information storing device which can at least be accessed by multiple members, and which is capable of storing a member list including public key information regarding members, a secret key list including encrypted key information, and encrypted data, and which employs the secret key cryptography and public key cryptography, wherein a secret key can be shared within at least a group, said method comprising the steps of:

a step for changing said member list in response to a member list manipulation request;

a step for registering a secret key for which a request has been made

to said secret key list in response to a registration request for a secret key, this registration including the encrypted key information of said secret key;

a step for selecting a secret key optimal for sharing information within a certain group at the time of the request, in response to the secret key request, and transmitting the selected secret key to the requesting destination;

a step for storing the encrypted data along with secret key information used for encrypting said data in response to the registration request of the encrypted data; and

a step for transmitting the relevant stored encrypted data and secret key information to the requesting destination in response to the request for obtaining encrypted data.

22. An information processing method for an information storing device according to Claim 21, further comprising a step for changing said member list and secret key list so that in the event of newly registering a member to a certain group, information shared by the group before the time of registration can be read.

23. An information processing method for an information storing device according to Claim 21, further comprising a step for changing said member list and secret key list so that in the event of deleting a member from a certain group, information shared by the group after the member is deleted cannot be read by the deleted member.

24. A computer-readable recording medium storing programs for causing a computer to execute the following steps:

a step for changing said member list in response to a member list manipulation request;

a step for registering a secret key for which a request has been made to said secret key list in response to a registration request for a secret key, this registration including the encrypted key information of said secret key;

a step for selecting a secret key optimal for sharing information within a certain group at the time of the request, in response to the secret key request, and transmitting the selected secret key to the requesting destination;

a step for storing the encrypted data along with secret key information used for encrypting said data in response to the registration request of the encrypted data; and

a step for transmitting the relevant stored encrypted data and secret key information to the requesting destination in response to the request for obtaining encrypted data.

25. A computer-readable recording medium storing programs for causing a computer to execute the following steps:

a step for changing said member list in response to a member list manipulation request;

a step for registering a secret key for which a request has been made to said secret key list in response to a registration request for a secret key, this registration including the encrypted key information of said secret key;

a step for selecting a secret key optimal for sharing information within a certain group at the time of the request, in response to the secret key request, and transmitting the selected secret key to the requesting destination;

a step for storing the encrypted data along with secret key information used for encrypting said data in response to the registration request of the encrypted data;

a step for transmitting the relevant stored encrypted data and secret key information to the requesting destination in response to the request for obtaining encryption data; and

a step for changing said member list and secret key list so that in the event of newly registering a member to a certain group, information shared by the group before the time of registration can be read.

26. A computer-readable recording medium storing programs for causing a computer to execute the following steps:

a step for changing said member list in response to a member list manipulation request;

a step for registering a secret key for which a request has been made to said secret key list in response to a registration request for a secret key, this registration including the encrypted key information of said secret key;

a step for selecting a secret key optimal for sharing information within a certain group at the time of the request, in response to the secret key request, and transmitting the selected secret key to the requesting destination;

a step for storing the encrypted data along with secret key information used for encrypting said data in response to the registration request of the encrypted data;

a step for transmitting the relevant stored encrypted data and secret key information to the requesting destination in response to the request for obtaining encrypted data; and

a step for changing said member list and secret key list so that in the event of deleting a member from a certain group, information shared by the group after the member is deleted cannot be read by the deleted member.

27. A computer-readable recording medium storing programs for causing a computer to execute the following steps:

a step for changing said member list in response to a member list manipulation request;

a step for registering a secret key for which a request has been made to said secret key list in response to a registration request for a secret key, this registration including the encrypted key information of said secret key;

a step for selecting a secret key optimal for sharing information within a certain group at the time of the request, in response to the secret key request, and transmitting the selected secret key to the requesting destination;

a step for storing the encrypted data along with secret key information used for encrypting said data in response to the registration request of the encrypted data;

a step for transmitting the relevant stored encrypted data and secret key information to the requesting destination in response to the request for obtaining encrypted data;

a step for changing said member list and secret key list so that in the event of newly registering a member to a certain group, information shared by the group before the time of registration can be read; and

a step for changing said member list and secret key list so that in the event of deleting a member from a certain group, information shared by the group after the member is deleted cannot be read by the deleted member.

28. An information tamper detection device having a sending terminal located at the sender side, and a receiving terminal located at the recipient side and connected with said sending terminal via a network, whereby information is sent and received between said sending terminal and receiving terminal, said information tamper detection device comprising:

a received contents confirmation data creation unit for creating received contents confirmation data indicating that said receiving terminal has confirmed reception of said information;

a sending unit for sending said received contents confirmation data via said network;

a receiving unit for receiving said receiving contents confirmation data via said network; and

a tamper detection unit which compares said information sent from said sending terminal with said receiving contents confirmation data, and detects tampering by the comparison results.

29. An information tamper detection device according to Claim 28, wherein said received contents confirmation data creation unit creates said receiving contents confirmation data based on one or a combination of a plurality of the following:

all or part of said information received by said receiving terminal;

a message digest consisting of all or part of said information digested by using Hash function;

sender information relating to the sender;

recipient information relating to the recipient; and

communication information.

30. An information tamper detection device according to Claim 28, wherein said receiving contents confirmation data creation unit creates said receiving contents confirmation data based on a message digest consisting of one or a combination of a plurality of the following, digested by using Hash function:

all or part of said information received by said receiving terminal;

a message digest consisting of all or part of said information digested by using Hash function;

sender information relating to the sender;

recipient information relating to the recipient; and

communication information.

31. An information tamper detection device according to Claim 28, wherein said receiving contents confirmation data creation unit creates said receiving contents confirmation data regarding one or a combination of a plurality of the following, bearing a digital signature:

all or part of said information received by said receiving side terminal;

a message digest consisting of all or part of said information digested by using Hash function;

sender information relating to the sender;

recipient information relating to the recipient; and

communication information.

32. An information tamper detection device according to Claim 28, wherein said receiving contents confirmation data creation unit

creates information consisting of one or a combination of a plurality of the following:

all or part of said information received by said receiving terminal;

a message digest consisting of all or part of said information digested by using Hash function;

sender information relating to the sender;

recipient information relating to the recipient; and

communication information;

creates a message digest comprised of said combination of information digested by using Hash function, and said combination of information bearing a digital signature; and

creates as the receiving contents confirmation data, a combination of two or more of the following:

said combination of information;

said message digest; and

said digital signed information.

33. An information tamper detection device having a sending terminal located at the sender side, and a receiving terminal located at the recipient side and connected with said sending terminal via a network, whereby information is sent and received between said sending terminal and receiving terminal, said information tamper detection device comprising:

a receiving contents confirmation data creation unit for creating receiving contents confirmation data indicating that said receiving terminal has confirmed reception of said information;

a transmitting unit for transmitting said receiving contents

confirmation data via said network;

a receiving unit for receiving said receiving contents confirmation data via said network; and

a computer-readable recording medium storing tampering-detection programs causing a computer to serve as a tamper detection unit which compares said information sent from said sending terminal with said receiving contents confirmation data, and detects tampering by the comparison results.

34. An information tamper detection device having a sending terminal located at the sender side, and a receiving terminal located at the recipient side and connected with said transmitting terminal via a network, whereby information is sent and received, said information tamper detection device comprising:

a receiving unit provided to said sending terminal, which receives received contents confirmation data via said network, said received contents confirmation information having been generated by said receiving terminal and indicating that said receiving terminal has confirmed reception of said information; and

a tamper detection unit provided to said sender side, which compares said received contents confirmation data received from said receiving unit with said information sent from said sending terminal, and detects tampering based on the comparison results thereof.

35. An information tamper detection device according to Claim 34, wherein said received contents confirmation data comprises information consisting of one or a combination of a plurality of the following:

all or part of said information received by said receiving terminal;

a message digest consisting of all or part of said information digested by using Hash function;

sender information relating to the sender;

recipient information relating to the recipient; and

communication information.

36. An information tamper detection device according to Claim 34, wherein said received contents confirmation data comprises information consisting of a message digest consisting of one or a combination of a plurality of the following, digested by using Hash function:

all or part of said information received by said receiving terminal;

a message digest consisting of all or part of said information digested by using Hash function;

sender information relating to the sender;

recipient information relating to the recipient; and

communication information.

37. An information tamper detection device according to Claim 34, wherein said received contents confirmation data comprises information consisting of one or a combination of a plurality of the following, bearing a digital signature:

all or part of said information received by said receiving terminal;

a message digest consisting of all or part of said information digested by using Hash function;

sender information relating to the sender;

recipient information relating to the recipient; and

communication information.

38. An information tamper detection device according to Claim 34, wherein said receiving contents confirmation data is created based on information consisting of one or a combination of a plurality of the following:

all or part of said information received by said receiving terminal;

a message digest consisting of all or part of said information digested by using Hash function;

sender information relating to the sender;

recipient information relating to the recipient; and

communication information;

is created as a message digest comprised of said combination of information digested by using Hash function, and said combination of information bearing a digital signature; and

comprises a combination of two or more of the following:

said combination of information;

said message digest; and

said digital signed information.

39. An information tamper detection device having a sending terminal located at the sender side, and a receiving terminal located at the recipient side and connected with said sending terminal via a network, whereby information is sent and received, said information tamper detection device comprising:

a receiving unit provided to said sending terminal, which receives received contents confirmation data via said network, said received contents

confirmation data having been generated by said receiving terminal and indicating that said receiving terminal has confirmed reception of said information; and

a computer-readable recording medium storing tampering-detection programs causing a computer to serve as a tamper detection unit provided to said sender side, which compares said reception contents confirmation information received from said receiving unit with said information sent from said sending terminal, and detects tampering based on the comparison results thereof.

40. An information tamper detection device having a sending terminal located at the sender side, and a receiving terminal located at the recipient side and connected with said sending terminal via a network, whereby information is sent and received between said sending terminal and receiving terminal, said information tamper detection device comprising:

a received contents confirmation data creation unit for creating receiving contents confirmation data indicating that said receiving terminal has confirmed reception of said information;

a sending unit for sending said received contents confirmation data via said network;

a receiving unit for receiving said received contents confirmation data via said network; and

a sent contents confirmation data creation unit which creates sent contents confirmation data based on said received contents confirmation data, indicating that the sending terminal has sent the information received by said receiving terminal, and sends the sent contents confirmation data to said receiving terminal via said network; and

a tamper detection unit which compares said sent contents confirmation data sent from said sent contents confirmation data creation unit with said information received by said receiving terminal, and detects tampering based on the comparison results.

41. An information tamper detection device according to Claim 40, wherein said sent contents confirmation data creation unit creates sent contents confirmation data based on one or a combination of a plurality of said received contents confirmation data and confirmation data indicating confirmation of the contents of said received contents confirmation data.

42. An information tamper detection device according to Claim 40, wherein said sent contents confirmation data creation unit creates sent contents confirmation data based on a message digest consisting of one or a combination of a plurality of said received contents confirmation data and said confirmation data, digested by using Hash function.

43. An information tamper detection device according to Claim 40, wherein said sent contents confirmation data creation unit creates sent contents confirmation data as one or a combination of a plurality of said received contents confirmation data and said confirmation data, with a digital signature.

44. An information tamper detection device according to Claim 40, wherein said sent contents confirmation data creation unit creates sent contents confirmation data based on a message digest consisting of one or a combination of a plurality of said received contents confirmation data and

said confirmation data, digested by using Hash function;

and wherein said sent contents confirmation data creation unit creates sent contents confirmation data as one or a combination of a plurality of said received contents confirmation data and said confirmation data, with a digital signature;

and wherein said sent contents confirmation data creation unit creates sent contents confirmation data based on a combination of two or more of the following:

said combination of information;

said message digest; and

said digital signed information.

45. An information tamper detection device having a sending terminal located at the sender side, and a receiving terminal located at the recipient side and connected with said sending terminal via a network, whereby information is sent and received, said information tamper detection device comprising:

a received contents confirmation data creation unit, provided to said receiving terminal, for creating received contents confirmation data indicating that said receiving terminal has confirmed reception of said data;

a sending unit, provided to said sending terminal, for sending said received contents confirmation data via said network; and

a tamper detection unit provided to said receiving terminal, which receives sent contents confirmation data via said network indicating that the information received by said receiving terminal has been transmitted, said sent contents confirmation data having been created by said sending terminal based on said received contents confirmation data, and which

compares said sent contents confirmation data with said information received from said receiving terminal, and which detects tampering based on the comparison results thereof.

46. An information tamper detection device according to Claim 45, wherein said sent contents confirmation data comprises one or a combination of a plurality of said received contents confirmation data and confirmation data indicating confirmation of the contents of said received contents confirmation data.

47. An information tamper detection device according to Claim 45, wherein said sent contents confirmation data comprises a message digest consisting of one or a combination of a plurality of said received contents confirmation data and said confirmation data, digested by using Hash function.

48. An information tamper detection device according to Claim 45, wherein said sent contents confirmation data comprises one or a combination of a plurality of said received contents confirmation data and said confirmation data, with a digital signature.

49. An information tamper detection device according to Claim 45, wherein said sent contents confirmation data is created based on a message digest consisting of one or a combination of a plurality of said received contents confirmation data and confirmation data indicating confirmation of the contents of said received contents confirmation data, digested by using Hash function;

and wherein said sent contents confirmation data is created as one or a combination of a plurality of said received contents confirmation data and said confirmation data, with a digital signature;

and wherein said sent contents confirmation data is created based on a combination of two or more of the following:

said combination of information;

said message digest; and

said digital signed information.

50. An information tamper detection device having a sending terminal located at the sender side, and a receiving terminal located at the recipient side and connected with said sending terminal via a network, whereby information is sent and received, said information tamper detection device comprising:

a received contents confirmation data creation unit, provided to said receiving terminal, for creating received contents confirmation data indicating that said receiving terminal has confirmed reception of said data;

a sending unit, provided to said sending terminal, for sending said received contents confirmation data via said network; and

a computer-readable recording medium storing tampering-detection programs causing a computer to serve as a tamper detection unit provided to said receiving terminal, which receives sent contents confirmation data via said network indicating that the data received by said receiving terminal has been sent, said sent contents confirmation data having been created by said sending terminal based on said received contents confirmation data, and which compares said sent contents confirmation data with said data received from said receiving terminal, and which detects tampering based on the

comparison results thereof.

51. An encryption device comprising a key encryption unit and an encryption unit;

said key encryption unit comprising:

a secret key obtaining unit for either obtaining or generating a secret key used for encryption employing the secret key cryptography;

a secret key encryption unit for encoding said secret key employing the public key cryptography so as to create an encrypted secret key; and

a first secret key tamper detection code creation unit for creating key information from said secret key, to be used for secret key tamper detection;

and said encryption unit comprising:

a data encryption unit for encrypting plain text using said secret key to create encrypted message; and

a first data tamper detection code creation unit for creating first data tamper detection code from said plain text.

52. An encryption device according to Claim 51, wherein said secret key encryption unit uses the public key for each user sharing encrypted message generated by said data encryption unit to encrypt said secret key and generate an encrypted secret key.

53. An encryption device according to Claim 51, said encryption device further comprising a key decryption unit;

said key decryption unit comprising:

a secret key decrypting unit for decrypting said encrypted secret key employing the public key cryptography;

a second secret key tamper detection code creation unit for creating secret key tamper detection code from the secret key obtained by decrypting said encrypted secret key; and

a first tamper detection unit for detecting tampering using said key information and said secret key tamper detection code;

wherein said key decryption unit verifies tampering as well as decrypts said encrypted secret key to obtain a secret key;

and wherein said encryption unit further encrypts additional plain text using said secret key.

54. A decryption device comprising a key decryption unit and a decryption unit for decrypting said encrypted secret key and said encrypted message encrypted by said encryption device according to Claim 51;

said key decryption unit comprising:

a secret key decrypting unit for decrypting said encrypted secret key by using the public key cryptography;

a second secret key tamper detection code creation unit for creating secret key tamper detection code from the secret key obtained by decrypting said encrypted secret key; and

a first tamper detection unit for detecting tampering using said key information and said secret key tamper detection code;

and said decrypting unit comprising:

a data decryption unit for decrypting encrypted message by using the secret key cryptography;

a second data tamper detection code creation unit for creating

second data tamper detection code from the plain text obtained by decrypting said encrypted message; and

a second tamper detection unit for detecting tampering using said first data tamper detection code and said second data tamper detection code.

55. A decryption device according to Claim 54, wherein said secret key decryption unit decrypts all encrypted secret keys corresponding with each user sharing encrypted message;

wherein said secret key tamper detection code creation unit creates said secret key tamper detection code for each secret key obtained by decrypting;

and wherein said first tamper detection unit detects tampering using said key information and said secret key tamper detection code, and also judges secret keys corresponding to users.

56. An encryption/decryption device comprising the encryption device according to Claim 51 and the decryption device according to Claim 54.

57. An encryption method, comprising:

a procedure for either obtaining or generating a secret key used for encryption employing the secret key cryptography;

a procedure for encoding said secret key employing the public key cryptography so as to create an encrypted secret key;

a procedure for creating key information from said secret key;

a procedure for encrypting plain text using said secret key to create

encrypted message; and

a procedure for creating first data tamper detection code from said plain text.

58. A decryption method, comprising:

a procedure for decrypting said encrypted secret key by employing the public key cryptography;

a procedure for creating secret key tamper detection code from the secret key obtained by decrypting said encrypted secret key;

a procedure for detecting tamper using said key information and said secret key tamper detection code;

a procedure for decrypting encrypted message by using the secret key cryptography;

a procedure for creating second data tamper detection code from the plain text obtained by decrypting said encrypted message; and

a procedure for detecting tamper using said first data tamper detection code and said second data tamper detection code.

59. A computer-readable recording medium storing programs for causing a computer to execute the following procedures:

a procedure for either obtaining or generating a secret key used for encryption using the secret key cryptography;

a procedure for encoding said secret key using the public key cryptography so as to create an encrypted secret key;

a procedure for creating key information from said secret key;

a procedure for encrypting plain text using said secret key to create encrypted message; and

a procedure for creating first data tamper detection code from said plain text.

60. A computer-readable recording medium storing programs for causing a computer to execute the following procedures:

a procedure for decrypting said encrypted secret key by using the public key cryptography;

a procedure for creating secret key tamper detection code from the secret key obtained by decrypting said encrypted secret key;

a procedure for detecting tampering using said key information and said secret key tamper detection code;

a procedure for decrypting encrypted message by using the secret key cryptography;

a procedure for creating second data tamper detection code from the plain text obtained by decrypting said encrypted message; and

a procedure for detecting tampering using said first data tamper detection code and said second data tamper detection code.

61. A team data list administration device for administration of team data lists for hierarchical ordering of a team, said device comprising:

an authentication unit for requesting operation of said team data list to a certain request destination, and according to the operation request, obtaining from the request destination the following for each team from the team which is the object of operation to the root team:

authority data including the identifier indicating the parent team of own team, and the digital signature of the administrator of said parent team; and

a team data list having an authority list including administrator information relating to authorized administration personnel of sub-teams under own team, and the digital signature of the team master which is the administrator of own team or the administrator of a parent team;

wherein confirmation is made for each team while backtracking the obtained team to said root team using said identifier, that there has been no tampering with the digital signature on said team data list and that the signature is that of one having authority, using said administrator information;

a team data list modification unit for modifying said team data list according to said operation request, once the validity thereof has been confirmed by said authentication unit; and

a signing unit for creating a digital signature of the individual instructing said operation request and attaching said digital signature said modified team data list, and sending this to said request destination.

62. A team data list administration device according to Claim 61, wherein said administration information comprises information relating to one or more sub-authorities which have been appointed from own team by said team master and have administrating authority over said sub-teams, and relating to said team master having administrating authority over said sub-authorities in addition to the authority of said sub-authorities.

63. A team data list administration device according to Claim 61, further comprising:

a registering unit for obtaining identification information for

performing identification of the team master of said root team and registering said identification information; and

a team master verification unit for using said identification information which has been pre-registered to verify that the digital signature of the authority data of said root team being sent from the request destination is the digital signature of the team master.

64. A team data list storing device for storing team data lists for hierarchical ordering of a team, said device comprising:

an authority data storing unit for storing, for each team, authority data including the identifier indicating the parent team of own team, and the digital signature of the administrator of said parent team;

an authority list storing unit for storing, for each team, an authority list having an authority list including administrator information relating to authorized administration personnel of sub-teams under own team, and the digital signature of the team master which is the administrator of own team or the administrator of a parent team; and

a permission test unit which uses said administrator information to confirm that the individual instructing said operation request from a certain request source to a team data list including at least said authority data and said authority list has request authority, wherein in the case of a reference request or deletion request, the requested team data list is returned to said request source or deleted, according to the reference request or deletion request, and wherein in the case of an update request, confirmation is made that the digital signature of the team data list sent from said request source is the signature of an individual having authority, thereby updating the stored contents of said authority data storing unit and said authority list

storing unit with the team data list that has been sent.

65. A team data list administration device according to Claim 64, wherein said administration information comprises information relating to one or more sub-authorities which have been appointed from own team by said team master and have administrating authority over said sub-teams, and relating to said team master having administrating privilege over said sub-authorities in addition to the privilege of said sub-authorities.

66. A team data list processing system having a team data list administration device according to one of the items in Claim 61 which is the request source, and the team data list storing device according to Claim 64 which is the request destination.

67. A recording medium, storing team data list administration programs for administration of team data lists for hierarchical ordering of a team, said programs causing a computer to execute the following processes:

a process for requesting operation of said team data list to a certain request destination;

a process for obtaining from the request destination the following for each team from the team which is the object of operation to the root team, according to the operation request:

authority data including the identifier indicating the parent team of own team, and the digital signature of the administrator of said parent team; and

a team data list having an authority list including administrator information relating to authorized administration personnel

of sub-teams under own team, and the digital signature of the team master which is the administrator of own team or the administrator of a parent team;

an authentication process for confirming each team while backtracking the obtained team to said root team using said identifier, that there has been no tampering with the digital signature on said team data list and that the signature is that of one having privilege, using said administrator information;

a modification process for modifying said team data list according to said operation request, once the validity thereof has been confirmed by said authentication process; and

a process for creating a digital signature of the individual instructing said operation request and attaching said digital signature to said modified team data list, and sending this to said request source.

68. A recording medium, storing team data list administration programs for administration of team data lists for hierarchical ordering of a team, said programs causing a computer to execute the following processes:

a process for storing beforehand, for each team, authority data including the identifier indicating the parent team of own team, and the digital signature of the administrator of said parent team;

a process for storing beforehand, for each team, an authority list having an authority list including administrator information relating to authorized administration personnel of sub-teams under own team, and the digital signature of the team master which is the administrator of own team or the administrator of a parent team; and

a permission test process which uses said administrator information

to confirm that the individual instructing said operation request from a certain request source to a team data list including at least said authority data and said authority list has request privilege, wherein in the case of a reference request or deletion request, the requested team data list is returned to said request source or deleted, according to the reference request or deletion request, and wherein in the case of an update request, confirmation is made that the digital signature of the team data list sent from said request source is the signature of a director having authority, thereby updating the stored contents of said authority data storing unit and said authority list storing unit with the team data list that has been sent.

69. A member list administration device in a broadcast communication system, said system comprising:

an encryption information creating device which creates code information including encrypted information formed by encrypting information to be sent;

a member list administration device performing administration of members lists including public keys of members to receive distribution of the broadcast;

an encrypted message decryption device which decrypts said encrypted message; and

a message broadcast device which receives encrypted message sent from said encrypted message creation device and distributes said encrypted message to one or more of said encrypted message decryption devices, based on said member list;

said member list administration device comprising:

a list creation unit for creating a member list including the

public key(s) of one or more members for broadcast communication; and

a public key administration unit for obtaining and saving said public keys.

70. A member list administration device according to Claim 69, further comprising a list retrieval and storing unit for retrieving and storing said member list either from a terminal via a network, or from a storage medium connected to the device.

71. A member list administration device according to Claim 69, further comprising a list transmitting unit for transmitting said member list via a network to a database connected to said network, said message broadcast device, or said encrypted message creation device or said encrypted message decryption device used by members included in said member list.

72. A member list administration device according to Claim 69, further comprising a subscription acceptor comprising:

a subscription request item setting unit for setting subscription request items for joining a broadcast communication member list; and

a subscription license judgement unit for judging whether or not the request items input and transmitted from the applicant satisfy said subscription request items, and whether or not subscription is admitted.

73. A encrypted message creation device in a broadcast communication system, said system comprising:

an encrypted message creation device which creates encrypted

message including encrypted information formed by encrypting information to be sent;

a member list administration device performing administration of members lists including public keys of members to receive distribution of the broadcast;

an encrypted message decryption device which decrypts said encrypted message; and

a message broadcast device which receives encrypted message sent from said encrypted message creation device and distributes said encrypted message to one or more of said encrypted message decryption devices, based on said member list;

said encrypted message creation device comprising:

a list retrieval and storing unit for retrieving and storing said member list either from a terminal via a network, or from a storage medium connected to the device; and

an encryption unit which obtains broadcast communication text, and encrypts said broadcast communication text using a public key included in said member list so as to form encrypted information.

74. A encrypted message creation device according to Claim 73, wherein said encryption unit creates an encrypted message of said broadcast communication text encrypted by the secret key cryptography, creates one or more encrypted secret keys of the secret key used in said secret key cryptography encrypted by the public key cryptography using one or more public keys included in said member list, creating key selection information for selecting encrypted secret keys corresponding to the members receiving distribution of the broadcast, and outputting said encrypted message, said

encrypted secret key, and said key selecting information, as said encrypted information.

75. An encrypted message creation device according to Claim 73, wherein, in the event that the broadcast communication text is composed of a plurality of components, said encryption unit performs encryption for each of the components making up said broadcast communication text and creates said encrypted information.

76. An encrypted message creation device according to Claim 73, further comprising a destination check unit for, in the event that the destination of the broadcast communication text is checked and said destination is said message broadcast device, and also in the event that a member list is obtained from said list retrieval and storing unit, sending said broadcast communication text to said encryption unit.

77. An encrypted message creation device according to Claim 73, further comprising a multiple parts sending unit for, in the event that the broadcast communication text is comprised of a main component and one or more dependent components, including reference information enabling reference to encrypted message corresponding to the dependent component to encrypted message corresponding to the main component and sending this to said message broadcast device, and sending encrypted message corresponding to the dependent components to an information storing device on the network.

78. An encrypted message decryption device in a broadcast

communication system, said system comprising:

an encrypted message creation device which creates encrypted message including encrypted information formed by encrypting information to be sent;

a member list administration device performing administration of members lists including public keys of members to receive distribution of the broadcast;

an encrypted message decryption device which decrypts said encrypted message; and

a message broadcast device which receives encrypted message sent from said encrypted message creation device and distributes said encrypted message to one or more of said encrypted message decryption devices, based on said member list;

said encrypted message decryption device further comprising:

an encrypted message retrieval unit for retrieving encrypted message transmitted from said message broadcast device; and

a decryption unit for decrypting the encrypted information included in said encrypted message.

79. An encrypted message decryption device according to Claim 78, said decryption unit comprising:

a key selection unit for making reference to key selection information included in said encrypted message, and selecting the encrypted secret key to be used for decryption;

an encrypted secret key decryption unit for decrypting with a private key of the recipient the encrypted secret key selected using the public key cryptography, thereby obtaining a secret key; and

an encrypted message decryption unit for decrypting the encrypted information included in said encrypted message using said secret key with the secret key cryptography, thereby obtaining the broadcast communication text in plain text.

80. An encrypted message decryption device according to Claim 78, said encrypted message decryption device further comprising a received notification transmitting unit for transmitting a received notification to said message broad cast device, thereby notifying that the member to receive the distribution has indeed received the same in person.

81. An encrypted message decryption device according to Claim 78, further comprising a multiple parts receiving unit for, in the event that the broadcast communication text is comprised of a main component and one or more dependent components, receiving encrypted message corresponding to the main component including reference information enabling reference to code information corresponding to the main component, and receiving encrypted message corresponding to the dependent components, based on said reference information.

82. An encrypted message decryption device according to Claim 78, further comprising a broadcast communication security checking unit for performing said checking according to one or a combination of the following:

checking of whether or not the member list used for creating encrypted message in said encrypted message creation device and the member list used for creating said distribution list are identical;

checking of whether or not the sender of encrypted message was

included in the member list;

checking of security regarding whether or not encrypted message has been tampered with along the communication path;

checking of whether or not there are malicious programs or data strings in transmitted information; and

checking of whether or not a part of encrypted message comprised of a plurality of parts created at the encrypted message creation device with reference to the transmitted encrypted message is being transmitted to another information storing device.

83. An encrypted message decryption device according to Claim 78, further comprising a list retrieval and storing unit for retrieving and storing said member list from a device already storing the member list, via a network.

84. An encrypted message decryption device in a broadcast communication system, said system comprising:

an encrypted message creation device which creates encrypted message including encrypted information formed by encrypting information to be sent;

a member list administration device performing administration of members lists including public keys of members to receive distribution of the broadcast;

an encrypted message decryption device which decrypts said encrypted information; and

a message broadcast device which receives encrypted message sent from said encrypted message creation device and distributes said encrypted

message to one or more of said encrypted message decryption devices, based on said member list;

said message broadcast device further comprising:

a destination list administration unit for performing administration of a destination list;

a message replication unit for replicating transmitted information; and

a transmitting unit for distributing the replicated encrypted message to each of the members to receive the distribution.

85. A message broadcast device according to Claim 84, wherein said destination list administration unit further comprises a list retrieval and storing unit which is capable of retrieving a members list from the location of storing whenever necessary, and storing said transmitted member list;

and changing said destination list so that information is distributed to the same set of members as the members included in the member list transmitted from the team master.

86. A message broadcast device according to Claim 84, further comprising a list authentication unit for automatically judging whether or not an digital signature is the signature of the valid team master, in the event that the validity of the digital signature attached to the member list is to be authenticated.

87. A message broadcast device according to Claim 84, further comprising an affixed information affixing unit for affixing an affixed information to all or a part of transmitted information.

88. A message broadcast device according to Claim 84, said message broadcast device further comprising a broadcast communication security checking unit for performing said checking according to one or a combination of the following:

checking of whether or not the member list used for creating encrypted message in said encrypted message creation device and the member list used for creating said destination list are identical;

obtaining received refusal information including the identification information of the receiving terminal or user refusing reception of information, checking whether or not the sender or sending terminal of information transmitted to the message broadcast device is included in said received refusal information;

checking of whether or not the sender of encrypted message was included in the member list;

checking of security regarding whether or not encrypted message has been tampered with along the communication path;

checking of whether or not there are malicious programs or data strings in transmitted information; and

checking of whether or not a part of encrypted message comprised of a plurality of parts created at the encrypted message creation device with reference to the transmitted encrypted message is being transmitted to another information storing device.

89. A message broadcast device according to Claim 84, further comprising a broadcast communication contents storing unit for storing the transmitted information or part of the transmitted information.

90. A message broadcast device according to Claim 84, further comprising a broadcast communication automatic start unit including:

a start request items presentation unit for presenting, on the terminal of the individual requesting start, the start request items which the individual requesting start should satisfy at the time of applying for start of broadcast communication service;

a start license judgement unit for judging whether or not the start application request transmitted by said individual requesting start satisfies the start request items, and whether start of broadcast communication service is to be permitted;

a broadcast communication start setting up unit, which, once start of broadcast communication service has been decided upon by said start license judgement unit, starts broadcast communication service wherein information is distributed to members specified by the team master, said individual requesting establishment being the team master.

91. A broadcast communication system, comprising:

a member list administration device according to Claim 69;

an encrypted message creation device according to Claim 73;

an encrypted message decryption device according to Claim 78; and

a message broadcast device according to Claim 84.

92. A computer-readable recording medium storing programs for causing a computer to execute the following procedures:

a procedure for creating a member list including the public key of at one or more members to which broadcast communication is to be conducted;

and

a procedure for retrieving and storing said public key.

93. A computer-readable recording medium storing programs for causing a computer to execute the following procedures:

a procedure for retrieving and storing a member list via a network; and

a procedure for retrieving the broadcast communication text, and encrypting said broadcast communication text using the public key included in said members list.

94. A computer-readable recording medium storing programs for causing a computer to execute the following procedures:

a procedure for obtaining encrypted message transmitted from said message broadcast device; and

a procedure for decrypting encrypted information included in said encrypted message.

95. A computer-readable recording medium storing programs for causing a computer to execute the following procedures:

a procedure for performing administration of the destination list;

a procedure for replicating transmitted encrypted message; and

a procedure for distributing the replicated encrypted message to the each member to receive distribution.

96. A team data list administration device, comprising:

a list creator verification unit for notifying a certain request

destination of information for performing personal identification/authentication regarding an individual instructing changes, the team data list which includes information relating to a team comprised of members mutually sharing resources and the digital signature of a master having administrative authority regarding said information and which has been prepared according to the authority of the members of the team is obtained from said request destination, and for confirming whether or not a master having authority created said team data list, based on the contents of said received team data list;

a list modification unit for modifying said team data list which has been confirmed to be a team data list created by said master having authority, according to said modifying instructions; and

a signing unit for creating a digital signature of the individual instructing the change, and affixing said digital signature to the modified team data list and sending said team data list to said request destination.

97. A team data list administration device according to Claim 96, said team data list comprising:

at least one member list including member information relating to said member and the digital signature of said master; and

a master list including master information indicating the privilege of said master and the digital signature of said master.

98. A team data list administration device according to Claim 97, wherein said master includes a team master having privilege to modify said master list, with said instruction to change being an instruction to change from said team master;

wherein said list creator verification unit verifies the digital signature of said member list at the transition state and master list at the transition state owing to being returned from said request destination corresponding to the member list and master list sent to said request destination and thereby changed;

and wherein said signature unit creates the digital signature of said master following the instructed modification owing to directive of modification, and returns the new member list and new master list formed by affixing said digital signature to said member list at the transition state and master list at the transition state.

99. A team data list administration device according to Claim 98, further comprising:

a registration unit for obtaining identification information for personal identification of said team master from a certain location, and registering said information; and

a team master verification unit for verifying whether or not the digital signature of said master is the digital signature of said team master, based on identification information of said team master, and the digital signature of said master included in said member list and said master list sent from said request destination.

100. A team data list administration device according to Claim 99, further comprising:

a modification verification unit for verifying that said team master has been modified by means of legal procedures, based on the modification in contents of the master list obtained at the time of said directive of

modification, the master list at said transition state, and said new master list; and

an identification information updating unit for obtaining identification information for the team master following the modification instructed by said directive to modify, and updating the identification information of the team master before the modification which is registered in said registration unit by identification information, with confirmation of said modification being a prerequisite to this operation of said identification information updating unit.

101. A team data list storing device, comprising:

a team data list storing unit for storing the team data list which includes information relating to a team comprised of members mutually sharing resources and the digital signature of a master having administrative privilege regarding said information and which has been prepared according to the authority of members of the team;

a first permission test unit for judging to a reference request from a certain request source, whether or not a director has the privilege for said request, based on said team data list and information for performing personal identification/authentication of said director who has made the request, and sending out said team data list only to request sources including said director having privilege; and

a second permission test unit for confirming the validity of a team data list in a modification request from said request source, based on the contents of the team data list sent from said request source, and for updating the stored contents of said time data list with the team data list regarding which the validity thereof has been confirmed.

102. A team data list storing device according to Claim 101, said team data storing unit comprising:

a member list storing unit for storing one or more member lists including at least member information relating to said members, and the digital signature of said master; and

a master list storing unit for storing a master list including at least master information indicating the authority of said master, and the digital signature of said master.

103. A team data list storing device according to Claim 102, wherein said master includes a team master having privilege to modify said master list, said second permission test unit further comprising:

a master list holding unit for holding the master list before a modification owing to a directive notified from said director to modify said team master, as a prior master list;

a portion for receiving from said request source the transitional master list and transitional member list in which information regarding said team master has been modified, out of said master list and said member list sent out to said request source by request of said request source, and detecting the modification in said team master based on these lists;

a portion for confirming the validity of the modification of said team master, based on said transitional master list and transitional member list as well as said prior master list, with detecting of said modification being a prerequisite to this operation; and

a portion for receiving the new master list and new member list to which is attached the digital signature of the post-modification chief master

specified by said directive of modification, as to the transitional master list and transitional member list sent out to said request source with confirmation of the validity thereof as a prerequisite, and for confirming the authority of these lists and modifying the stored contents of said member list storing unit and said master list storing portion.

104. A team data list processing system, comprising:

a team data list administration device according to Claim 96 which is the request source; and

a team data list storing device according to Claim 101, which is the request destination.

105. A computer-readable recording medium storing team data list administration programs for causing a computer to execute the following procedures:

a process for notifying a certain request destination of information for performing personal identification/authentication regarding a director of the modifications, the team data list which includes information relating to a team comprised of members mutually sharing resources and the digital signature of a master having administrative authority regarding said information and which has been prepared according to the privilege of the members of the team is obtained from said request destination;

a processing for confirming whether or not a master having privilege created said team data list, based on the contents of said received team data list;

a list modification process for modifying said team data list which has been confirmed to be a team data list created by said master having

privilege, according to said modification directive; and

a signing process for creating a digital signature of the director of the modification, and affixing said digital signature to the modified team data list and sending said team data list to said request destination.

106. A computer-readable recording medium storing team data list administration programs for causing a computer to execute the following procedures:

a process for storing the team data list which includes information relating to a team comprised of members mutually sharing resources and the digital signature of a master having administrative privilege regarding said information and which has been prepared according to the authority of members of the team;

a process for judging whether or not a director of a reference request from a certain request source has the privilege for said request, based on said team data list and information for performing personal identification/authentication of the director who has made the request, and sending out said team data list only to request sources including a director having privilege; and

a permission test process for testing the permission of a team data list in a modification request from said request source, based on the contents of the team data list sent from said request source, and for updating the stored contents of said time data list with the team data list regarding which the validity thereof has been confirmed.